

**REMARKS/ARGUMENTS**

This communication is responsive to the Non-Final Office Action of June 27, 2005 in which the following objections were raised: [4] Applicant's claim for domestic priority under 35 U.S.C. 119(e) is acknowledged; [5] Claims 9 and 11 are objected to because of informalities requiring correction.; [3,6,7] Claims 1-18 was rejected under 35 U.S.C. 103(a) as being unpatentable over Brodersen USP: 6,732,100 in view of Win USP: 6,453,353.

Applicant has canceled Claims 2, 5-7, 13 and 15-17 and amended remaining Claims 1, 3-4, 8-12, 14, 18.

**(5) CLAIMS 9, 11 OBJECTED TO DUE TO INFORMALITIES**

Claims 9 and 11 are objected to because of informalities requiring correction, specifically the limitation "further for entering" requires correction.

Applicant has amended Claims 9 and 11 to overcome the objection and requests that such objection be withdrawn.

**(3,6,7) CLAIMS 1-18 REJECTED UNDER 35 U.S.C. 103(a):**

Claims 1-18 was rejected under 35 U.S.C. 103(a) as being unpatentable over Brodersen USP: 6,732,100 in view of Win USP: 6,453,353.

The Applicant has amended all remaining Claims including Independent Claims 1, 14 and 18.

The Bordersen reference discloses two types of database schema in the sole figures accompanying the reference. FIG. 1 shows a very high level view of what is identified as a 'multi-organization support' database schema and FIG. 2 shows a very high level view of what is identified as a 'multi-tenant' database schema. (Brodersen at col 4 lines 29-30 and col 6 lines 7-8). *"In the multi-tenancy embodiment, the access is typically triggered by an incoming call to a vendored call center, and the view is based on the customer's computer*

*telephony integration (CTI)-identified account number. Similarly, in the multi-organization support embodiment, the access is triggered by end user action, and the specific view is triggered by the end-user's logon, that is, which division or channel or reporting chain is used for this task.*" (Brodersen at col 3 line 67 to col 4 line 9). Mention is made in the sections cited by the Examiner of the visibility of data associated with a view determined by the user's organization and also by the position of the user within the organization. Nowhere however in the reference is there any indication that the visibility of data to a user is handled dynamically by the manager of a group as is the case in the Applicant's invention, rather visibility or lack thereof appears to be 'hard-coded' into a view of the database.. *"The common vendor stores the merchants' and institutions' customer accounts in an access controlled database...computer-telephony integration...automatically switches the agent to the correct slice (that is, customer files) of the database."*(Brodersen at Col 5 lines 57-67).

With the exception of a database the Brodersen reference is devoid of any of the key limitations of Applicant's amended Claims. The Brodersen reference does not disclose any web pages let alone a group registration web page for entering a registration record of a new group including a group identifier and a user identifier for a user having a role of group manager for the new group or a managerial web page for each group manager to manage registration records for users and roles for each user within the group manager's associated group. Neither does the Brodersen reference disclose an application with an access controller whereby a plurality of group managers each determine for their associated group both the users in their group and the data records of the group accessible to each user both of which are claimed limitations of the Applicants amended Independent Claim 1.

The Win reference discloses a system which *"enables administrators to implement access rules by defining Roles that Users play when working for an organization or doing business with an enterprise."* (Win at col. 5, lines 21-22). The Win system includes an administrative application for controlling a Registry Repository of users, resources and roles. (Win at col. 5, lines 19-20) and runtime modules on each protected server in the enterprise. The runtime modules use the information in the registry repository to determine whether a resource is protected and if so whether or not a requesting user should have access to it. *"When a Runtime Module ... is notified of a change by the Administration Application... the Runtime Module ...to read updated information from the Registry Server."* (Win at col 7 lines

64-67). The Runtime Module uses this information to determine when a requested URL is a protected resource and conditions access accordingly. (Win at col 8 lines 15-17) .

Win also discloses a decentralized access control. But the access control is not truly decentralized relying on manual delegation by a Super Administrator to one or more users in the enterprise accorded limited administrative roles manually assigned by the Super Administrator. *"The system is installed with a 'super user' or 'SuperUser Administrator' account that is assigned an Admin Role with Configuration Privileges and System Administration Privileges. The super user account can be used to configure, populate and maintain a system. In particular, the super user account can be used to delegate administration by creating Admin Role records and assigning them to user records."*(Col. 17, lines 14-20). *"....An example of an Admin Role is 'Help Desk Administrator'. An enterprise might have a dozen such administrators located at various sites of the enterprise".*"(Col. 16, lines 5-12) .

Win's administrative application runs on a dedicated workstation rather than within an application as is the case with the Applicant's claimed invention. (Win at col. 12 lines 61-63). The Win reference specifically teaches away from incorporation of access control into an application itself. *"In the past, users have had to log in individually to each Web application that they are authorized to use. In the preferred embodiment, users always access the same login page regardless of the number of resources to which they need access. Thus, the system provides a mechanism of single secure log-in to Web resources."*(Win at Col. 6, lines 3-9)

Thus neither the Win nor the Brodersen reference singly or in combination disclose or suggest an application with an access controller which is part of an application whereby a plurality of group managers each determine for their associated group both the users in their group and the data records of the group accessible to each user both of which are claimed limitations of the Applicants amended Independent Claims.

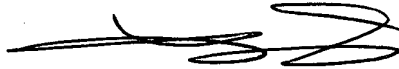
The Applicant therefore respectfully submits that Independent Claims 1, 14 and 18 have been amended to overcome the rejection based on either or both the Win and Brodersen references. The Applicant therefore respectfully requests that the Examiner withdraw this rejection. Remaining Claims depend directly or indirectly from corresponding ones of the amended Independent Claims 1, 14 and 18 and thus are also believed to have been amended

into a form suitable for withdrawal of the rejection for the reasons discussed above and for other reasons of independent significance.

## CONCLUSION

In view of the above remarks, and the amendments to all remaining Claims Applicant respectfully submits that Claims 1, 3-4, 8-12, 14, 18 have been placed in a condition for allowance, and requests that they be allowed. Early notice to this effect is solicited.

Respectfully submitted,



Liping Zhang  
Registration No. 45,520

Date: December 27, 2005

10171 Macadam Lane  
Cupertino, CA 95014  
Tel: (408) 252-1860  
Fax: (408) 252-1860